6750-01-P]

FEDERAL TRADE COMMISSION

[File No. 192 3126]

Ascension Data & Analytics, LLC; Analysis to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed Consent Agreement; Request for Comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order—embodied in the consent agreement—that would settle these allegations.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER]*.

ADDRESSES: Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Please write "Ascension Data & Analytics, LLC; File No. 192 3126" on your comment, and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Jarad Brown (202-326-2927), Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR § 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Website at this web address: https://www.ftc.gov/news-events/commission-actions.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. Write "Ascension Data & Analytics, LLC; File No. 192 3126" on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

Because of the public health emergency in response to the COVID-19 pandemic and the agency's heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the *https://www.regulations.gov* website.

If you prefer to file your comment on paper, write "Ascension Data & Analytics, LLC; File No. 192 3126" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580; or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D),

Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov*, you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website—as legally required by FTC Rule 4.9(b)—we cannot redact or remove your comment from that

website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at http://www.ftc.gov to read this Notice and the news release describing the proposed settlement. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

Analysis of Proposed Consent Order to Aid Public Comment

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Ascension Data & Analytics, LLC ("Respondent"). The proposed consent order ("Proposed Order") has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission again will review the agreement and the comments received, and will decide whether it should withdraw from the agreement or make final the agreement's Proposed Order.

Respondent is a Delaware company with its principal place of business in Texas. Respondent provides data, analytics, and technology services to other companies in its corporate family and their service providers relating to residential mortgages.

In early 2017, as part of work for a related company, Respondent hired a vendor to conduct Optical Character Recognition on a set of documents pertaining to 37,000 residential mortgages. The documents contained the personal information of 60,593 consumers. The type of personal information included names, dates of birth, Social

Security numbers, loan information, credit and debit account numbers, drivers' license numbers, and credit files. Before providing the documents to the vendor, Respondent did not take steps to make sure the vendor was capable of protecting the personal information in the documents. Furthermore, Respondent did not require the vendor by contract to protect the documents or the consumer information contained therein.

From January 2018 to January 2019, the vendor inadvertently exposed the information from the mortgage documents online, by misconfiguring a cloud server and storage location containing information from the documents. As a result, anyone who could figure out the web address of the server or storage location could view and download the contents. he server and storage location were accessed by fifty-two unauthorized computers during the year they were exposed.

The Commission's proposed one-count complaint alleges that Respondent violated the Standards for Safeguarding Customer Information Rule ("Safeguards Rule") of the Gramm-Leach-Bliley Act ("GLB Act"). The Safeguards Rule requires financial institutions, which includes companies like Respondent, to implement a comprehensive information security program that contains certain elements.

The proposed complaint alleges that Respondent violated the Safeguards Rule by failing to include two of the required elements in its information security program. First, the proposed complaint alleges, Respondent did not oversee service providers, by failing to take reasonable steps to choose service providers capable of safeguarding personal information, and failing to require those service providers by contract to maintain the safeguards. Second, the proposed complaint alleges, Respondent failed to identify risks to the security of personal information, and assess whether any safeguards it had in place were sufficient. Respondent did not satisfy this element of the Safeguards Rule because it failed to consider risks related to many service providers, and did not conduct risk assessments before September 2017.

The Proposed Order contains provisions designed to prevent Respondent from engaging in the same or similar acts or practices in the future. Part I of the Proposed Order prohibits Respondent from violating the Safeguards Rule.

Part II of the Proposed Order requires Respondent to establish and implement, and thereafter maintain, a comprehensive data security program that protects the security of Covered Information, the definition of which is modeled off the definitions of the Safeguards Rule. Part III of the Proposed Order requires Respondent to obtain initial and biennial data security assessments for ten years. Part IV of the Proposed Order requires Respondent to disclose all material facts to the assessor and prohibits Respondent from misrepresenting any fact material to the assessments required by Part III. Part V of the Proposed Order requires Respondent to submit an annual certification from a senior corporate manager (or senior officer responsible for its data security program) that Respondent has implemented the requirements of the Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part VI of the Proposed Order requires Respondent to notify the Commission any time it is required to make a notification to a state or local government that personal information has been breached or disclosed. Parts VII through X of the Proposed Order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide information or documents necessary for the Commission to monitor compliance. Part XI states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to aid public comment on the Proposed Order. It is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify in any way the Proposed Order's terms.

By direction of the Commission, Commissioner Chopra dissenting, Commissioner Slaughter not participating.

April J. Tabor,

Acting Secretary.

Statement of Commissioner Noah Joshua Phillips Regarding Ascension Data & Analytics, LLC

The Commission today announced our most recent settlement resolving an alleged violation of the Gramm-Leach-Bliley Safeguards Rule ("Rule"), a critical facet of the Commission's data privacy and security enforcement program. According to the complaint, Ascension Data & Analytics ("Ascension") violated the Rule by failing to vet properly and oversee a provider of optical character recognition (OCR) services, and by failing to conduct appropriate risk assessments. This settlement requires Ascension to implement a comprehensive data security program including annual third-party assessments.

I write to address several points in Commissioner Chopra's dissenting statement. Commissioner Chopra dissents because he believes the Commission should name Rocktop Partners, a company in the same corporate family as Ascension, as a respondent. Commissioner Chopra points to corporate affiliation and certain overlaps in management and facilities between the two firms, and other entities as well. It is not clear under what legal theory—whether veil piercing, common enterprise, or the like—he would name other defendants; but, without more, the facts alleged do not support doing so.[1]

[1] For example, Commissioner Chopra cites no facts to suggest that corporate formalities were not observed, that Ascension is under-capitalized, or that corporate form was abused to inoculate Rocktop from liability (mind the reader, for Ascension's failure to oversee a vendor) to justify piercing the corporate veil. Courts generally take a dim view of piercing the corporate veil without a substantial basis to do so. *See, e.g., Trinity Indus., Inc. v. Greenlease Holding Co.*, 903 F.3d 333, 365 (3d Cir. 2018) ("the corporate veil may be pierced only in extraordinary circumstances, such as when the corporate form would otherwise be misused to accomplish certain wrongful purposes") (internal citations and quotations omitted). And for

In terms of relief, Commissioner Chopra argues that Rocktop will dissolve Ascension and set up a new firm or transfer its functions, just to avoid its obligations under the settlement. This is the kind of conduct characteristic of boiler rooms and other frauds. It is not clear to me why Rocktop—an entity regulated by the Securities and Exchange Commission—would dissolve and reconstitute an affiliate for the sole purpose of failing to oversee vendors, or otherwise evading this order.[2]

Commissioner Chopra also would have the Commission allege that Ascension's conduct was unfair. In the Gramm-Leach-Bliley (GLB) Act, Congress gave us a specialized data security statute, and the Safeguards Rule, promulgated pursuant to that Act, establishes liability under the facts alleged in this case.[3] We should use that authority, and here we are. I do not see what an additional allegation of unfairness would achieve—certainly, no change in the remedy, and nothing better for consumers. What is more, when pleading that lax data security was unfair under Section 5, we need evidence to satisfy the unfairness test; that gets into thornier questions of whether the oversight failure here can constitute unfairness. Thanks to GLB, we need not answer that.

Commissioner Chopra claims that Ascension is being favored because, in the Commission's 2014 case against GMR Transcription Services, it pleaded an unfairness count. He attributes the difference in treatment to the small size of the respondent in that case. GMR was not a financial services firm, however, so the Commission could not have alleged a violation of the GLB Safeguards Rule in that case; and the respondent in this

---

good reason: the ability to make investments without risk of liability is foundational to the American legal and economic system.

[2] Commissioner Chopra cites *FTC v. Wyndham Worldwide Corp*., No. 2:13-cv-01887 (ES), 2014 WL 2812049, at *8 (D.N.J. June 23, 2014), for the proposition that companies other than frauds may reorganize in an effort to avoid responsibilities under FTC orders. Of course that is true, but that does not mean that every entity in a corporate family can or should be bound by every FTC order. And, certainly, that is not what the court—considering a motion to dismiss—held in that case.

[3] 15 U.S.C. 6801 *et seq*; 16 CFR part 314. The limits of applying Section 5 to data security cases are precisely why the Commission, on a bipartisan basis, seeks data security legislation from Congress.

case, Ascension, is also a small company. It is not at all unusual for the Commission to charge a violation of the Safeguards Rule without an accompanying unfairness count.[4]

This is a strong case and a good result. I commend Staff for its thoughtful and energetic efforts to use the authority at our disposal to protect American consumers.

Dissenting Statement of Commissioner Rohit Chopra Regarding Ascension Data & Analytics, LLC [Redacted]

Summary

- After an egregious data breach involving extremely sensitive financial information, the Commission has struck a settlement that provides no help for victims and does little to deter.
- It appears Ascension Data & Analytics is really just an offshoot of a large investment fund, and the Commission's proposed order fails to bind the appropriate parties.
- To achieve meaningful results, the Commission must reevaluate its enforcement strategy when it comes to safeguarding consumer financial information by working collaboratively with other regulators and applying its unfairness authority in an even-handed manner.

Americans have been burned by the mortgage industry before – not just by slipshod practices that maximize profits at the expense of responsible stewardship, but also by slippery accountability when things go wrong. Regulators got lost in a labyrinth

[4] *See, e.g., TaxSlayer, LLC*, No. C-4626 (Nov. 8, 2017), https://www.ftc.gov/enforcement/cases-proceedings/162- 3063/taxslayer; *James B. Nutter & Co.*, No. C-4258 (June 16, 2009), https://www.ftc.gov/enforcement/casesproceedings/072-3108/james-b-nutter-company-corporation-matter; *United States v. American United Mortgage Co*., No. 07-cv-7064 (N.D. Ill.), https://www.ftc.gov/enforcement/cases-proceedings/062-3103/american-united-mortgagecompany-united-states-america-ftc. I am unaware of any case where we alleged a failure to oversee as a violation of both GLB and Section 5, as Commissioner Chopra would have us do here.

of shell companies and subsidiaries, and too many who profited escaped unscathed, leaving families in ruin.

To achieve the dream of homeownership, Americans typically have to fork over a boatload of personal data to mortgage lenders, like our Social Security numbers, our driver's license numbers, our pay stubs, and more. This is the norm when you borrow to buy a home. The lender then transfers this data onward through the financial system, with banks, servicers, mortgage funds, investment vehicles – and their vendors – all gaining access. This data, in the wrong hands, is valuable intelligence not only for identity thieves but also for nation states, leading to threats to our financial and national security. That's why federal law ensures that financial institutions have safeguards in place to secure this highly sensitive data.

After a data breach of highly sensitive data from mortgage applications, the FTC launched an investigation into Ascension Data & Analytics. Ascension worked on behalf of its sister companies, such as investment funds to analyze mortgages. Ascension also hired other vendors to help. Even though Ascension was required under the law to guard consumer financial data, in fact, they were using third parties with shoddy security, as alleged in the complaint. Given the breadth and sensitivity of the data compromised in this breach, an individual consumer would probably prefer to be affected by the Equifax breach than this one, if forced to make a choice.

In my view, the Commission's proposed resolution of this investigation suffers from three key flaws: It fails to hold all of the right parties accountable. It fails to charge unfair conduct as unfair. And it fails to redress consumers or deter other firms from engaging in similar misconduct.

Ascension, Rocktop Partners, and Corporate Musical Chairs

Ascension is not really an independent company.[1] It's in the same corporate family as Rocktop Partners,[2] a multi-billion dollar private equity fund that buys up defective mortgages, such as those with title disputes.[3] Ascension's President, Brett Benson, is also Managing Director of Rocktop Partners.[4] Its office sits on the same floor as Rocktop Partners at 701 Highlander Boulevard in Arlington, Texas.[5] When the Ascension breach hit the news, it was Rocktop's General Counsel, Sandy Campbell, who confirmed the key details of the incident.[6] It is unclear whether Ascension has any clients other than Rocktop Partners or others in its corporate family.[7] This is a common arrangement in finance, since it allows fund managers to profit when they can bill their investors for services.

Further, Rocktop's Managing Director and Chief Financial Officer, Jonathan Bray, is also the sole person ("manager" or "member") listed on the LLC forms for a firm called Reidpin LLC.[8] Langhorne Reid and Jason Pinson ("Reid" and "Pinson") are cofounders of Rocktop.[9] Unsurprisingly, Reidpin LLC is located at the same address as Ascension and Rocktop.[10] It is therefore clear that Ascension is anything but arms-length from Rocktop. Rocktop's corporate structure confirms this conclusion:

Figure 1: [Redacted]

The FTC has charged Ascension Data & Analytics – but not any other parties in the broader Rocktop family – with violating the Safeguards Rule by failing to police its agents processing personal data. I agree that Ascension violated the law, but I am

---

[1] My office has endeavored to cite public sources showing a portion of the web of companies involving Ascension, Rocktop, and Reidpin LLC.
[2] Zack Whittaker, *Millions of bank loan and mortgage documents have leaked online*, TECHCRUNCH (Jan. 23, 2019), https://techcrunch.com/2019/01/23/financial-files/.
[3] ROCKTOP PARTNERS, https://rocktoppartners.com/ (last visited on Oct. 2, 2020).
[4] *Id*.
[5] *Id*., Compl., In the Matter of Ascension Data & Analytics, LLC, Fed. Trade Comm'n File No. 1923126.
[6] *Supra* note 2.
[7] *Id*.
[8] Reidpin, LLC, Application to Register a Foreign Limited Liability Company (LLC) (Nov. 17, 2020) https://businesssearch.sos.ca.gov/Document/RetrievePDF?Id=201816410221-24379676.
[9] *Supra* note 3.
[10] *Supra* note 8.

concerned that the proposed settlement will do little to prevent future failures. In addition, our complaint and the Analysis to Aid Public Comment would be strengthened with critical information about the Rocktop corporate structure.[11]

The FTC's order binds only one company: Ascension. The company that actually appears to manage more than $7 billion worth of Americans' mortgages – Rocktop – is not being required to change a single thing about its practices.[12] And while Ascension will be required to clean up its act, nothing is stopping the controllers of Rocktop from creating a "new" analytics firm staffed with exactly the same executives, or even transferring the functions within their corporate family, but without any obligations under the FTC's order. This would be economically rational. The Commission does not cite any sworn testimony or other evidence to show why they believe the controllers of Ascension would act irrationally.

Commissioner Phillips argues that this is a concern in cases involving "boiler rooms and other frauds." I respectfully disagree. When the FTC charged Wyndham in 2012 with lax data security practice, it named not only the parent corporation but also three subsidiaries, alleging that they operated with common control, shared offices, overlapping staff, and as part of a maze of interrelated companies. Defending these charges against dismissal, the Commission argued that "[i]f the Court were to enter an order against only [the subsidiary], Wyndham would be able to transfer responsibility for data security to another Wyndham entity[,]" allowing the company to sidestep its obligations under any order.[13] The court agreed, specifically rejecting the view that only "shell companies designed to perpetrate fraud" can face charges.[14]

---

[11] Commissioner Phillips points to the fact that Rocktop Partners may be a registered investment fund under the securities laws, but does not discuss the other entities within the corporate family and in any related mortgage vehicles that are not.

[12] *Supra* note 3.

[13] *Fed. Trade Comm'n v. Wyndham et al*., 2013 WL 11116791 (D.N.J. May 20, 2013).

[14] *Fed. Trade Comm'n. v. Wyndham Worldwide Corp*., 2014 WL 2812049, at *7 (D.N.J. June 23, 2014).

The FTC should not be allowing companies to evade accountability through a game of corporate musical chairs. An effective order would bind not only Ascension, but also all of the parties liable under the law. While one of these parties may be outside the jurisdiction of the FTC's Safeguards Rule, there is no question that they are bound by the FTC Act's prohibition on unfair practices.

Unfair Conduct is Unlawful, Regardless of Size

The FTC has declined to include a charge of violating the FTC's prohibition on unfair practices. This represents a departure from previous cases involving similar misconduct, and raises questions as to whether the FTC is engaging in disparate treatment based on business size and type, rather than on facts and evidence.

In 2014, the FTC charged Ajay Prasad, Shreekant Srivastava, and their company, GMR Transcription Services, with violating the FTC Act's prohibition on unfair practices when it failed to ensure its vendors protected sensitive data. As detailed in the Commission's complaint, GMR failed to ensure that their vendors implemented reasonable security measures, and failed to prevent one vendor from storing sensitive files in plain text. The complaint does not allege that malicious actors attacked the vendor's systems, nor does it allege that GMR's failure to oversee the vendor directly led to the improper data disclosure, but nevertheless charges both the firm and its owners with engaging in unfair business practices by failing to employ reasonable security measures.[15]

If GMR faced this scrutiny, why wouldn't Ascension? The FTC's complaint alleged that GMR's lax policies created a vulnerability that was exploited at least once, and the FTC's complaint in this matter details some of the consequences of this catastrophic breach, which involved dozens of actors, mainly from overseas, including those with IP addresses in China and Russia. They were able to access more than 60,000

---

[15] Compl., *In the Matter of GMR Transcription Services, Inc*., Fed. Trade Comm'n File No. 1223095 (Aug. 21, 2014), https://www ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf.

Americans' sensitive financial information. Furthermore, in failing to prevent this mass theft, Ascension disregarded its own risk management policies, failing to take "any of the steps described in its own policy to evaluate [its vendors'] security practices."[16]

Taken together, the allegations against Ascension leave little doubt that the company's practices were unfair, causing far more unavoidable injury than GMR, without any apparent benefit to consumers or competition.[17] When the Commission settled with GMR, the law was exactly the same. The only thing that changed is the five members of the Commission.

My colleague suggests there are questions about whether Ascension's practices were unfair, but the Commission's complaint details how elementary the missteps were that led to this breach. A reasonable person would expect if these problems could have been prevented simply by Ascension following its own vendor management policies. Ascension could have also heeded the FTC's 2015 business guidance, which warns firms to "[m]ake sure service providers implement reasonable security measures."[18]

My colleague also cites instances where the Commission has charged a firm with violating the FTC's Safeguards Rule without also including charges of unfair practices. However, these cases do not involve conduct related to inadequate service provider oversight, which is the core allegation at issue with Rocktop and Ascension.

We must apply more evenhanded enforcement to ensure that large businesses and investment firms are not getting less scrutiny than small businesses. The Commission's failure to charge Ascension and its affiliates with an unfairness violation is not only inconsistent with prior practice but also undermines our ability to hold the company accountable for its failures.

---

[16] Compl., *In the Matter of Ascension Data & Analytics, LLC*, Fed. Trade Comm'n File No. 1923126.

[17] *See* 15 U.S.C. 45n, defining as unfair those practices that cause or are likely to cause substantial injury that is not reasonably avoidable, and is not outweighed by benefits to consumers or competition.

[18] START WITH SECURITY, A GUIDE FOR BUSINESS, LESSONS LEARNED FROM FTCC CASES, FED. TRADE COMM'N (Jun. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

Rethinking Remedies

The most effective way to address serious data breaches like this one is to compensate the victims, penalize the wrongdoers, and insist on changes to the responsible company's practices. Unfortunately, the Commission's proposed order misses the mark on identifying the responsible company, while doing nothing to compensate victims or penalize those responsible for this catastrophic breach. I am therefore not confident that the remedies proposed in today's order will deter other companies from engaging in the same slipshod practices.

We could have done more. I recognize that consumers harm can be difficult to estimate in these cases, and that the Commission lacks civil penalty authority for offenses like this one. But that problem can be solved. The FTC is not the only enforcer in this space – dozens of state attorneys general and financial regulators can enforce a nearly identical unfairness authority under federal law that is backed up with strong tools to both seek redress and penalties. By partnering with a state enforcer, the Commission can dramatically improve its data security actions – ensuring that there is compensation for victims and consequences for wrongdoing.[19]

Unfortunately, the FTC almost never invites state regulators, particularly state banking regulators with significant expertise, to join our investigations and enforcement actions to obtain additional relief when it comes to data protection. This must change.

Conclusion

We should all be unconvinced that chasing after dangerous data breaches and resolving them without any redress or penalties is an effective strategy. Making matters worse, holding a "company" accountable that is really just an extension of a financial firm might allow our order to be completely ignored. After this settlement, Ascension

---

[19] In addition to having unfairness jurisdiction, many state enforcers have their own versions of the Safeguards Rule. *See, e.g.*, *Industry Guidance Re: Standards for Safeguarding Customer Information and Regulation 173*, NEW YORK STATE DEP'T OF FIN. SERV., https://www.dfs ny.gov/insurance/ogco2002/rg204021.htm.

could "fold," and the Rocktop family of companies can reconstitute it, escaping any obligations under the order.[20]

The FTC is currently considering changes to its rule on safeguarding consumer financial information.[21] But we also need to rethink our enforcement strategy. Our go-it-alone strategy is doing nothing for breach victims and little to deter, and our two-track approach to unfairness is penalizing small companies while giving a pass to financial firms like Rocktop. For these reasons, I respectfully dissent.

[FR Doc. 2020-28407 Filed: 12/22/2020 8:45 am; Publication Date: 12/23/2020]

[20] For context, public information indicates that there are seven companies with interrelated officers or agents currently active, including "Reidpin LLC," "Reidpin, LLC," "Reidpin Investments, LLC," Reidpin Rocktop 1, LLC," "Reidpin Rocktop III, LLC," "Reidpin Rocktop IV, LLC," "Reidpin Rocktop V, LLC" founded in 2011, 2014, 2015, 2016, two in 2017, and one in 2018. There are two other entities with these characteristics which appear to have folded. https://opencorporates.com/companies?q=REIDPIN%2C+LLC.

[21] Fed. Trade Comm'n., Standards on Safeguarding Customer Information, 84 FR 13158 (Apr. 4, 2019), https://www federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information.